1215417

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 22, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/482,786*
FILING DATE: *June 25, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/20562*

Certified by

Jon W Dudas

Acting Under Secretary of Commerce
for Intellectual Property
and Acting Director of the U.S.
Patent and Trademark Office

PTO/SB/16 (10-01)
Approved for use through10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

11749 U.S. PTO
60/482786
06/25/03

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No.	EU245162794US

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Lance M.	Cottrell	San Diego, California
James A	Reynolds	Carlsbad, California
Darya	Mazandarany	San Diego, California

☑ Additional inventors are being named on the 1 separately numbered sheets attached hereto

TITLE OF THE INVENTION (500 characters max)

A MULTIPLE PLATFORM NETWORK PRIVACY SYSTEM

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ Customer Number _____ → Place Customer Number Bar Code Label here

OR Type Customer Number here

☑ Firm or Individual Name	Francisco A. Rubio-Campos				
Address	The Eclipse Group				
Address	26895 Aliso Creek Road, Suite B-104				
City	Aliso Viejo	State	CA	ZIP	92656
Country	USA	Telephone	949-448-9410	Fax	714-948-8903

ENCLOSED APPLICATION PARTS (check all that apply)

☑ Specification	Number of Pages 13	☐ CD(s), Number	
☑ Drawing(s)	Number of Sheets 4	☐ Other (specify)	
☐ Application Data Sheet. See 37 CFR 1.76			

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

		FILING FEE AMOUNT ($)
☐	Applicant claims small entity status. See 37 CFR 1.27.	
☑	A check or money order is enclosed to cover the filing fees	
☑	The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 502542	$80.00
☐	Payment by credit card. Form PTO-2038 is attached.	

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____ Date 06/25/2003

TYPED or PRINTED NAME Francisco A. Rubio-Campos

REGISTRATION NO. (if appropriate) 45,358

TELEPHONE (949) 448-9410

Docket Number: IF03002USV

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

PROVISIONAL APPLICATION COVER SHEET
Additional Page

PTO/SB/16 (02-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Docket Number	IF03002USV

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family or Surname	Residence (City and either State or Foreign Country)
Gene Nelson	Nelson	Spring Valley, California
Robert Torres	Torres	Chula Vista, California

Number 2 of 2

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

PTO/SB/17 (05-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 80.00

Complete if Known	
Application Number	Unknown
Filing Date	June 25, 2003
First Named Inventor	Lance M. Cottrell et al.
Examiner Name	Not applicable
Art Unit	Unassigned
Attorney Docket No.	IF03002USV

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☑ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 502542

Deposit Account Name: The Eclipse Group

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☐ Charge any additional fee(s) during the pendency of this application

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	750	2001	375	Utility filing fee	
1002	330	2002	165	Design filing fee	
1003	520	2003	260	Plant filing fee	
1004	750	2004	375	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	80.00

SUBTOTAL (1) ($) 80.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X =
Independent Claims		- 3** =		X =
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	84	2201	42	Independent claims in excess of 3
1203	280	2203	140	Multiple dependent claim, if not paid
1204	84	2204	42	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	410	2252	205	Extension for reply within second month	
1253	930	2253	465	Extension for reply within third month	
1254	1,450	2254	725	Extension for reply within fourth month	
1255	1,970	2255	985	Extension for reply within fifth month	
1401	320	2401	160	Notice of Appeal	
1402	320	2402	160	Filing a brief in support of an appeal	
1403	280	2403	140	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,300	2453	650	Petition to revive - unintentional	
1501	1,300	2501	650	Utility issue fee (or reissue)	
1502	470	2502	235	Design issue fee	
1503	630	2503	315	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	750	2809	375	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	750	2810	375	For each additional invention to be examined (37 CFR 1.129(b))	
1801	750	2801	375	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY

Name (Print/Type)	Francisco A. Rubio-Campos	Registration No. (Attorney/Agent)	45,358	(Complete *(if applicable)*) Telephone	949-448-9410
Signature				Date	June 25, 2003

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

U.S. Express Mail No.: EU245162794US
Filing Date: June 25, 2003

PATENT
Docket No. IF03002USV

A MULTIPLE PLATFORM NETWORK PRIVACY SYSTEM

INVENTORS

LANCE M. COTTRELL
JAMES A REYNOLDS
DARYA MAZANDARANY
GENE NELSON
&
ROBERT TORRES

BACKGROUND OF THE INVENTION

[001] **1. Field of the Invention.**

[002] This invention relates generally to network communication systems. In particular, this invention relates to an Internet privacy system capable of operating across multiple platforms.

[003] **2. Related Art.**

[004] As the global computer network known as the Internet continues to grow globally at a rapid pace, an increasing number of people and businesses from around the world are accessing the Internet for both business and personal activities. As a result, the Internet has become a virtual community were people communicate with each other by sending and receiving electronic, voice and image messages for business and pleasure. These communications include sharing ideas and information, sending personal and business message back and forth, researching information, expressing opinions and ideas both personal and political, and conducting business negotiations and transactions (generally known as "electronic commerce" or "e-commerce"). In response to this new

electronic activity, business, governments and certain individuals attempt to identify and track individual Internet users for numerous purposes including, but not limited to, advertising, market research, customizing information of Internet sites (i.e., "websites") snooping and ease dropping on communications, political and law enforcement activities, fraud and malicious activities. Many of these attempts are threats to the individual users of the Internet because they attempt to gain personal information about the user and the user's activities on the Internet (generally referred to as the user's "online activities") typically without the user's express consent or knowledge.

[005] These threats typically gain information about the user by logging a user's Internet Protocol ("IP") address (the electronic address that specifically identifies a user's computer to the network) or by installing programs or files on to the user's computer such as "cookies," ActiveX™ applications, Java™, script files, Spyware, or hostile programs such as viruses. These threats allow an outside user, be it a government, business, or individual entity, to perform such tasks as identify a user, obtaining the user's personal information that is stored on the computer (including names, address, financial, private files, and/or other confidential, private and/or sensitive information), and track the user's activities on the Internet including recording every website visited or every email sent or received by the user. Malicious programs such as viruses may also be installed on the user's computer that can modify, erase or destroy the user's operating system of personal files.

[006] Unfortunately, most people that utilize the Internet do not understand technically how networks such as the Internet function nor do they generally appreciate

the number and types of threats that they will experience once they connect (i.e., "log-on") to the Internet. Past attempts at protecting users on the internet include using "firewalls" to block certain types of threats from the Internet, virus protection programs for detecting malicious programs, and spyware and cookie file removal software. However, these past attempts do not protect a user's identity because most of these approaches attempt to disinfect a user from intruders after the fact. These past approaches do not protect a user's identity as soon as the user connects to the Internet because connected websites are able to read and identify the user's IP address among other things. A need therefore exist to protect a user's identity as soon as the user connects to the Internet (i.e., known as "surfing the web" or "surfing the Net").

[007] Attempts in the past at protecting the user's identity have included allowing a user to connect to an intermediate server connected to the Internet that extracted off the user's IP information and substituted it with the IP address of the intermediate server thus creating an anonymous user that could then continue to surf the Net without worrying that their IP information would be used to identify them.

[008] Unfortunately, this approach was too technical and difficult to operate by most Internet users. Therefore, there is a need for a privacy management system that solves the problems recited above and allows Internet users to easily maintain their privacy by utilizing an anonymous server.

BRIEF DESCRIPTION OF THE FIGURES

[009] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[010] FIG. 1 shows a flow-chart of an example of a startup process for the AnonPro Web Server Startup Wizard Support Script.

[011] FIG. 2 shows a flow chart of an example process for Key Validation.

[012] FIG. 3 shows a flow chart for an example process of account creation.

[013] FIG. 4 shows a flow-chart for an example process preformed by an AnonPro Web-Server Logon/Authentication Module.

DETAILED DESCRIPTION

[014] This invention describes a method for providing Internet privacy service which shall be described in relation to example implementation herein referred to as AnonPro. AnonPro may be a specific implementation of our inventions for providing Internet privacy services. The components described in this detailed description and figures are an example implementation for some of our particular applications, however, the technologies and inventions described herein are much more general. The components are generally a network level traffic interceptor (client side), a client proxy, a server proxy, an SSL module, and some web based services (such as the user authentication, server lists, recommended site settings lists etc.). Generically speaking, the combination of the components is an "Internet privacy system." The client part is

"Internet Privacy Client", while the server proxy is "Internet Privacy remote proxy." In the description of this invention we often refer to registry entries or other specific ways of storing information. In all cases this information could be stored in any number of ways including in flat files, indexed files, local or remote databases, among others. In the description of this invention we often refer to cookies. Many other information transfer techniques could be used in place of cookies including HTML headers, changes to URLs or other addresses, any other standard or custom message or data structure. In the description of this invention we often refer to XML data structures. In general these structures could be replaced with any other kind of data structure, including other standard and non-standard, encrypted and non-encrypted structures. CA stands for "Certificate Authority" and refers to an entity or encryption key used for signing other keys such as SSL keys.

Additionally, The AnonPro Server Proxy (also known as the "Internet Privacy Remote Proxy") is a system that relays data from the client on the user's PC to the computer hosting the content or service the user is trying to access through the system's Internet Privacy System (the Destination). The proxy acts to hide the user's IP address and may perform other actions based on the content of the request or the contents of the reply from the Destination. These actions may include adding, changing, or removing text, data, information, scripts or other content from either the data from the user to the destination, or from the destination back to the user. The Internet Privacy Remote Proxy is not used in all modes of the Internet Privacy Client. In some modes the Internet Privacy Client connects directly to the Destination. Whether or not the Internet Privacy Remote Proxy is

used depends on the privacy settings the user has set for that particular site. The Internet Privacy Remote Proxy is only used if the hiding of the user's IP, or the other changes the Remote Proxy makes to the data, are required for the particular settings. Otherwise the connection is direct.

[015] This is summarized listing of the modules that may be included in the AnonPro Web-Server development. FIG. 1 shows a flow-chart of an example of a startup process for the AnonPro Web Server Startup Wizard Support Script. The process that may be a CGI script written in PERL. Its general purpose is to interface with the AnonPro client application Startup Wizard Module. The AnonPro client may make HTTPS posts to this script when the Startup Wizard Module is called. This script should determine the action to take based upon an "action" parameter.

[016] FIG. 2 shows a flow chart of an example process for Key Validation. When the AnonPro Web Server Startup Wizard Support Script receives an action parameter it may perform Key Validation. The first step of key validation may be reading in the registration key from the a parameter. The script may reference a database to find out if this key exists in the registration key table. Existence in this table will determine that this is a valid registration key. If the key exists in the database the edition that is associated with it may be retrieved as well. If this key has been previously used, it may lookup the public key that is associated with the registration key. It may then return the edition and public key to the client with the status of "used". If the key has not been previously used the script may generate a public key and store it in the database. It may then return the edition, public key, and a status of "new".

[017] FIG. 3 shows a flow chart for an example process of account creation. The account creation section may handle the creation, renewal, or reinstallation of the user's account. Account creation may be performed when an unused key is passed in with a valid and available username and password. The user may be inserted into the necessary tables in order to allow the user to use the AnonPro service. Account renewal may be performed when an unused key is passed in with the username and password of an existing user. The user's account may be then updated to reflect the upgrade in service determined by the registration key. Account reinstallation may be performed when the user is not creating a new account or upgrading/renewing an existing account, but is merely trying to activate an installation of the AnonPro client.

[018] FIG. 4 shows a flow-chart for an example process preformed by an AnonPro Web-Server Logon/Authentication Module. The AnonPro Web Server Login Script may handle user authentication for the AnonPro client. The AnonPro client may make a silent HTTPS post to the Login Script. In this post the AnonPro client may pass in the username and password of the user to be authenticated. This script may determine the status of the user and set the necessary cookies in order for the user to be able to use the AnonPro service.

[019] As an example of operation, the AnonPro Web-Server Logon/Authentication Module script first the checks to determine whether sure the uname ("username")and passwd ("password") parameters have been passed in. If they are not passed in, it checks for the existence of an APMeta-Auth cookie. The username and password would then be extracted from the APMeta-Auth cookie and the script would proceed as normal. In the

event that the username and password are not passed in and there is no APMeta-Auth cookie, the script may return an "invalid" status and exit.

[020] The script then connects to the Anonymizer database and searches for a user with the given username and password. If a user is not found with the given information the script may return a status of "invalid". If the user is found, the script then checks to see if the user has an active AnonPro account. If the user does not have an AnonPro account or has an expired AnonPro account the script may return the status of "expired" (When the AnonPro client receives an "expired" status it should inform the user.). If the user owns an account that is not expired for some other reason is not active, the script may return a status of "inactive".

[021] If it has been determined that the user has an active AnonPro account it may proceed in setting the necessary authorization cookies. The APAuth cookie is what the AnonPro Proxy Servers may check in order to authenticate the user. It typically has approximately a two-hour lifetime. It typically contains the type of service of the user's account, the possibly encrypted username, the timestamp for expiration (epoch time), and a hash which verifies the authenticity of the cookie. The APMeta-Auth cookie may allow the AnonPro Proxy servers the ability to redirect to the Login Script and receive authentication without interaction with the AnonPro client. The APMeta-Auth cookie may contains the encrypted username and the uid (i.e., "user id") of the user.

[022] The processes described in may be performed by hardware or software. If the process is performed by software, the software may reside in software memory (not shown) in the controller, memory, or an removable memory medium. The software in

memory may include an ordered listing of executable instructions for implementing logical functions (i.e., "logic" that may be implement either in digital form such as digital circuitry or source code or in analog form such as analog circuitry or an analog source such an analog electrical, sound or video signal), may selectively be embodied in any computer-readable (or signal-bearing) medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that may selectively fetch the instructions from the instruction execution system, apparatus, or device and execute the instructions. In the context of this document, a "computer-readable medium" and/or "signal-bearing medium" is any means that may contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer readable medium may selectively be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples "a non-exhaustive list" of the computer-readable medium would include the following: an electrical connection "electronic" having one or more wires, a portable computer diskette (magnetic), a RAM (electronic), a read-only memory "ROM" (electronic), an erasable programmable read-only memory (EPROM or Flash memory) (electronic), an optical fiber (optical), and a portable compact disc read-only memory "CDROM" (optical). Note that the computer-readable medium may even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance optical scanning of the paper or other medium, then compiled, interpreted or

otherwise processed in a suitable manner if necessary, and then stored in a computer memory.

[023] In general, the system described provides for Consensual Man in the Middle Attack by using used to rewrite pages, on the fly creation of site SSL certificates, CA cert to sign all SSL site certificates, CA cert is generated per user, CA cert is automatically installed in the browser and SSL page rewriting. Where the SSL page rewriting included the Client decrypting SSL pages to rewrite before re-encrypting and sending to proxy or end web site.

[024] The system also provides for the Client to Insert information into data stream from browser to Internet through any kind of Header or by inserting cookies. The cookies may include authentication / access rights information and preferences information and utilize XML and encryption.

[025] The system may also provides for a TCP level hook for privacy service that includes the Hook redirecting traffic to a local proxy on the user's machine, the Client proxy redirecting traffic to Anonymizer proxy and the TCP hook allows IP hiding.

[026] The system may also provides for a Full time SSL without URL prefixing.

[027] The system may also provides for making cookies session only and/or change cookie expiration date.

[028] The system may also provides for gathering and generation Privacy Statistics that include Per site privacy statistics, a Privacy Analyzer real time threat display, and automated site threat analysis and rating.

[029] The system may also provides for setting per site privacy settings that include white lists, black lists, detailed custom settings, "Show details" functionality, recommended site settings list that include automatically updated and downloaded settings, and hard coded Site settings that can't be changed by user have preset defaults and an exception list for some sites.

[030] The system may also provides for the Client to keep a list of alternate access names / IP addresses for accessing servers. The Client may tries all addresses one after another and/or each user gets a different set of access addresses.

[031] The system may also provides allows install on many computers while detect and prevent multiple simultaneous users.

[032] The system may also provides allows Client Javascript [script] rewriting. The system utilizes a novel GUI design to manage information.

[033] While various embodiments of the application have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. Accordingly, the invention is not to be restricted except in light of the attached claims and their equivalents. The foregoing description of an implementation has been presented for purposes of illustration and description. It is not exhaustive and does not limit the claimed inventions to the precise form disclosed. Modifications and variations are possible in light of the above description or may be acquired from practicing the invention. For example, the described implementation includes software but the invention may be implemented as a combination of hardware and software or in hardware

alone. Note also that the implementation may vary between systems. The claims and their equivalents define the scope of the invention.

CLAIMS

What is claimed is:

1. A method for allowing a user to connect to a privacy network comprising:

connecting to the network;

receiving a user name and password from a user; and

determining whether the user account is valid.

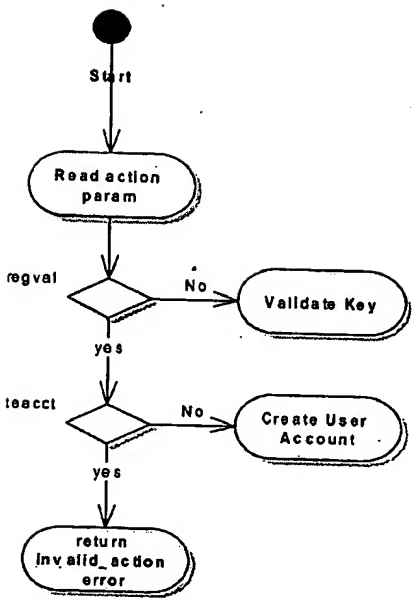
Start
Read action param
regval
No
Validate Key
yes
teacct
No
Create User Account
yes
return invalid_action error

FIG. 1

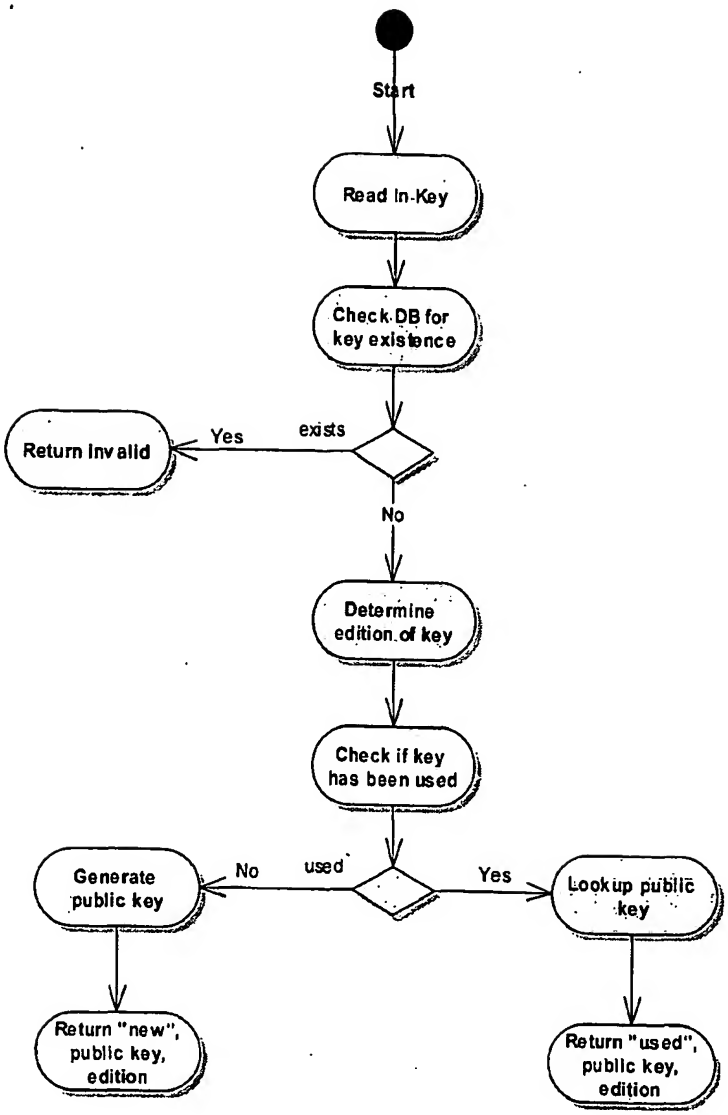
Start
Read In-Key
Check DB for key existence
exists
Yes
Return Invalid
No
Determine edition of key
Check if key has been used
used
No
Yes
Generate public key
Lookup public key
Return "new", public key, edition
Return "used", public key, edition

FIG. 2

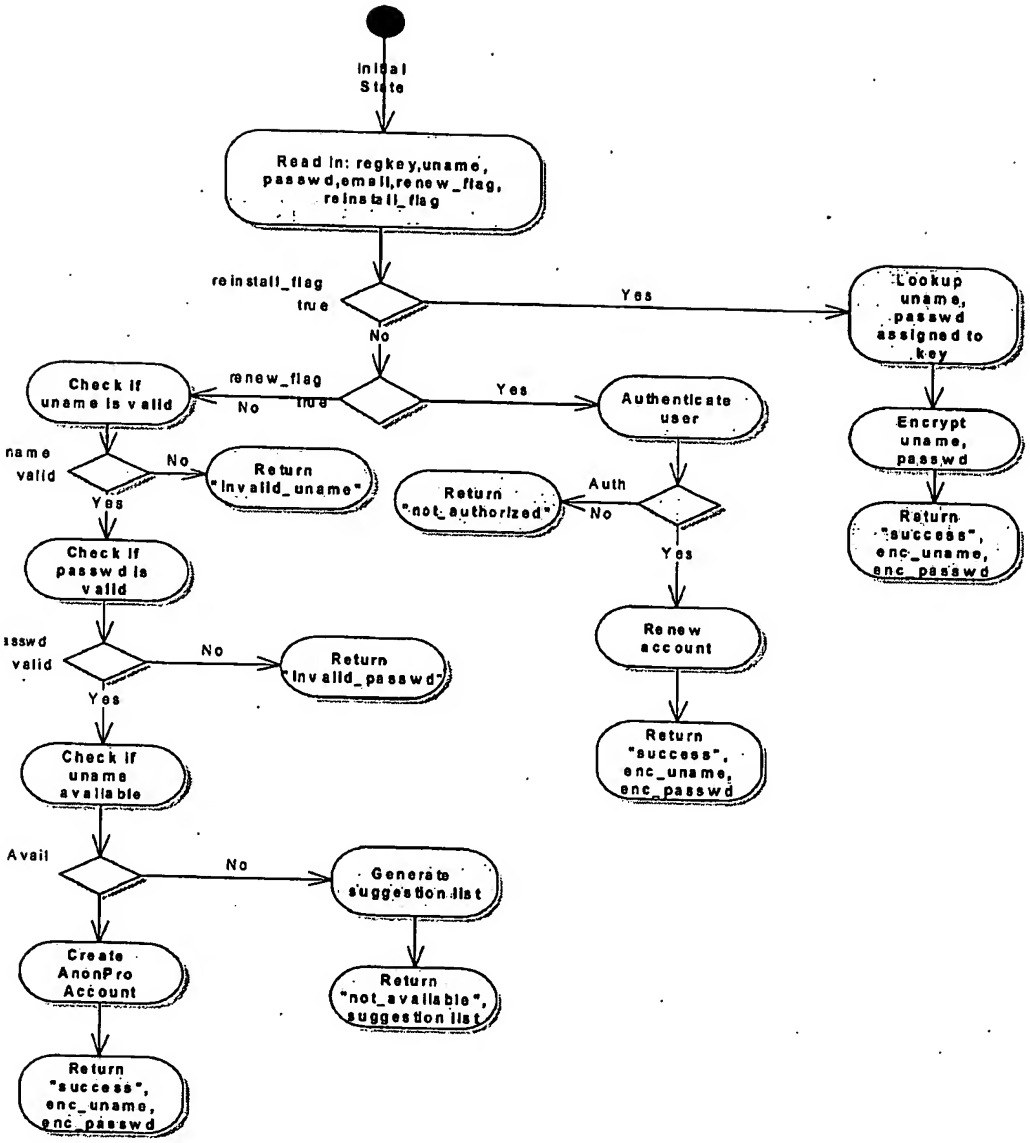
Initial State
Read In: regkey,uname, passwd,email,renew_flag, reinstall_flag
reinstall_flag true
Yes
No
Lookup uname, passwd assigned to key
Encrypt uname, passwd
Return "success", enc_uname, enc_passwd
renew_flag true
No
Yes
Check if uname is valid
Authenticate user
name valid
No
Yes
Return "invalid_uname"
Return "not_authorized"
Auth
No
Yes
Check if passwd is valid
Renew account
sswd valid
No
Yes
Return "invalid_passwd"
Return "success", enc_uname, enc_passwd
Check if uname available
Avail
No
Yes
Generate suggestion list
Return "not_available", suggestion list
Create AnonPro Account
Return "success", enc_uname, enc_passwd

FIG. 3

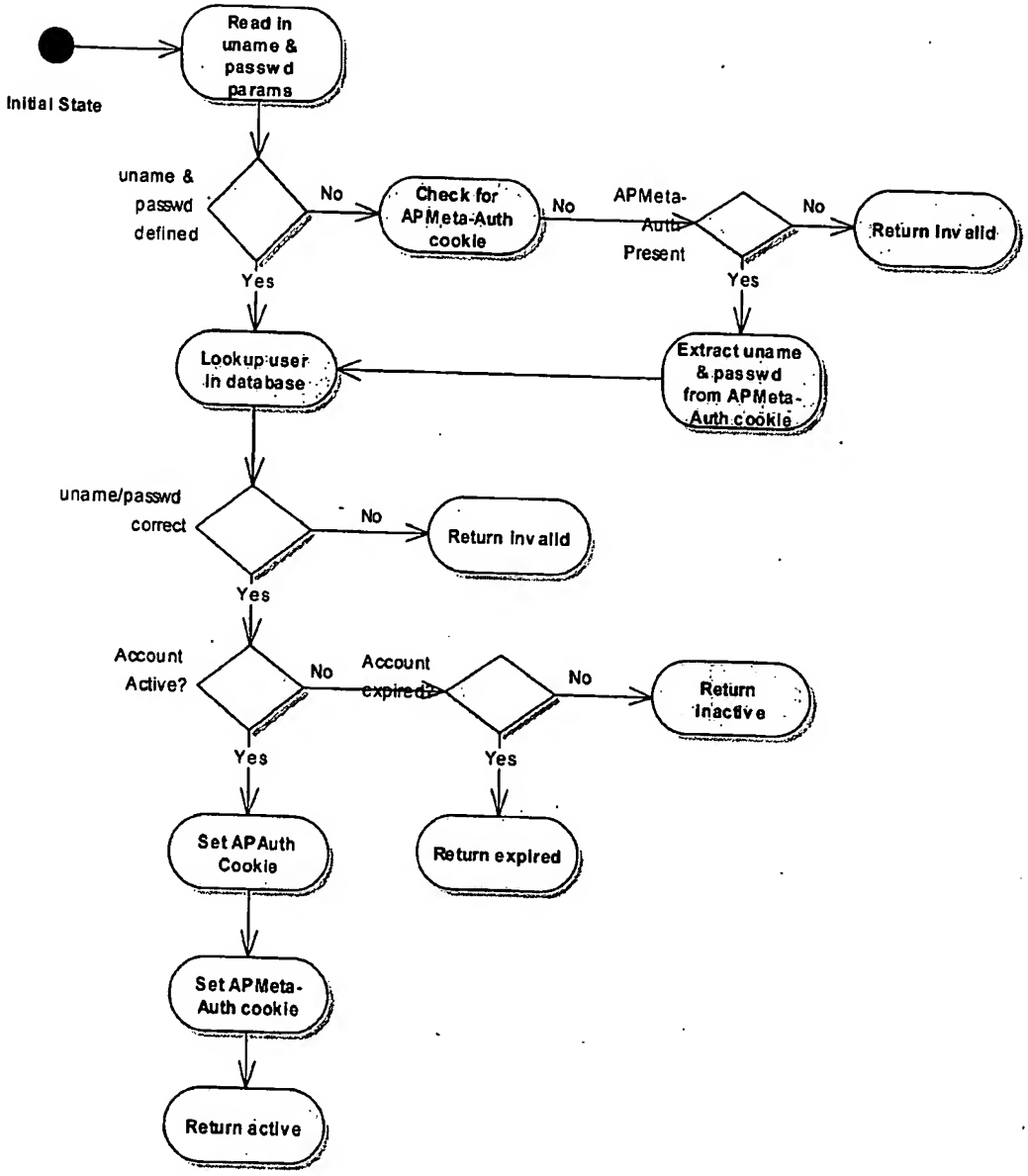
Initial State
Read in uname & passwd params
uname & passwd defined
No
Yes
Check for APMeta-Auth cookie
No
APMeta-Auth Present
No
Yes
Return Invalid
Lookup user in database
Extract uname & passwd from APMeta-Auth cookie
uname/passwd correct
No
Yes
Return Invalid
Account Active?
No
Yes
Account expired?
No
Yes
Return Inactive
Set APAuth Cookie
Return expired
Set APMeta-Auth cookie
Return active

FIG. 4

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/020562

International filing date: 25 June 2004 (25.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/482,786
Filing date: 25 June 2003 (25.06.2003)

Date of receipt at the International Bureau: 02 September 2004 (02.09.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse